Health Information Technology Standards Committee
Final Summary
Of the November 30, 2010, Meeting

KEY TOPICS

1. Call to Order

Judy Sparrow, Office of the National Coordinator (ONC), welcomed participants to the 19th meeting of the HIT Standards Committee (HITSC), which was conducted as a virtual meeting. She reminded Committee members that this was a Federal Advisory Committee meeting, with an opportunity for the public to make comments. She conducted roll call, and turned the meeting over to National Coordinator for Health Information Technology David Blumenthal.

2. Opening Remarks

David Blumenthal noted that Phase 1 of meaningful use will go fully live with the physician community on January 1. He expressed his interest in learning about how this first stage of meaningful use will be used, perceived, and practically implemented. As the HITSC pursues the discussion about what meaningful use Stage 2 will look like—at first generally and then with increasing specificity—the Committee will be working closely with the HIT Policy Committee (HITPC) to ensure that policy is implementable from a standards perspective.

3. Review of the Agenda

HITSC Chair Jonathan Perlin reviewed the agenda, noting that much of the discussion at this meeting would focus on mechanisms for sharing health information and standards for routing health information data. He asked Committee members if they had any revisions to the draft minutes of the last HITSC meeting, which was held on October 27, 2010. Cammie Roberts asked that an addition be made on page 3 of the draft summary. During the October meeting, she was asked a question and immediately after the meeting, she e-mailed the answer to Committee members.

Co-Chair John Halamka noted that significant rollouts have been seen within the last 6 months. The Committee has not yet identified transport standards intentionally, recognizing that this process is an evolution. There is a risk that 50 different transport mechanisms, all of which are incompatible, could be established. The NHIN Connect and the Direct Project are working towards convergence on this issue. The HITSC will need to evaluate the Direct Project and ask whether it has met the goal of creating simple, direct, and secure transport. John Halamka noted that testimony from this meeting will provide a valuable foundation for evaluating the Direct Project. He characterized transport as the last great gap in achieving interoperability in this country, and getting to what is needed for Stages 2 and 3.

> **Action Item #1:** Minutes from the last HITSC meeting, held on October 27, 2010, were approved by consensus with the addition Cammie Roberts' e-mailed response to Committee members.

4. Workgroup Updates

Implementation Workgroup

Implementation Workgroup Chair Liz Johnson reported that the group is convening a hearing on the topic of real-world experiences working with meaningful use. The hearing will be held on January 10-11, 2011. The Implementation Workgroup also is working with Doug Fridsma and the HITPC Certification/Adoption Workgroup to align their efforts.

John Halamka noted that they move from Stage 1 to Stages 2 and 3, the Centers for Medicare and Medicaid Services (CMS) and the ONC are seeking a large amount of feedback on the standards and meaningful use measures. He suggested that if the CMS and ONC learn that there are significant struggles over the course of the first 6 months of 2011, it may substantially influence the aggressiveness and pace of Stages 2 and 3. Hearing from those engaged in these activities who are "in the trenches" is key. Another critical aspect is ensuring that HITSC recommendations are reflective of what is happening and what is possible.

Clinical Operations Workgroup

John Halamka indicated that one topic the Clinical Operations Workgroup would like to pursue centers around device standards. As health care reform becomes a reality, there may be more home care and more distributed use of devices. These devices must have the right content, vocabulary, and transmission standards. In the first quarter of 2011, hearings are planned to further address these device standards.

Privacy and Security Workgroup

Dixie Baker had no update from the Workgroup, but did comment that during the testimony at this meeting, Committee members should remember to examine transport devices from the home to the provider entity. Nancy Orvis suggested that the Workgroup clarify the types of medical devices to which it wants to apply standards. In addition to monitoring electronic medical devices, consideration also must be given to creating medical summaries that include implantable devices and durable medical equipment such as walkers, artificial limbs, etc. John Derr added telemedicine to the list of considerations, noting the importance of monitoring devices to home care and nursing homes.

5. Vendor Discussion on Standards for Routing Health Information Data and Reaction From HITSC Members, Arien Malec, NHIN Direct, and Doug Fridsma, ONC

John Halamka noted that on the day prior to this meeting, the Direct Project issued a press release describing its success in the creation of an implementation guide, in running code, and in garnering support from the vendor community. Hundreds of stakeholders have been approached and asked to look at how REST, SOAP, SMTP, and various other transport options will work or not, so that any small provider can get information to any other small provider. At this meeting, stakeholders will provide information on point-to-point push transactions.

Peter Tippett, Verizon

Just over 1 year ago, Verizon started building Verizon Medical Data Exchange and announced in March 2010 that an exchange was running with eight vendor users, including content management groups, electronic medical record (EMR) companies, and transcription companies. The exchange can support any document type and does not require a specific document structure. The original functionality of the exchange that was developed is a machine-to-machine exchange, using RESTful protocol.

A few weeks ago, Verizon added a portal that would allow humans to join the exchange, and by January, it intends to make free accounts available for 2.3 million doctors, nurse practitioners, and physicians assistants, all of whom are part of a directory. Verizon will also be issuing X509 credentials for signing or identity. This credential would allow people to use standard identities that chain up to worldwide root certificates, and therefore could be used by any platform.

Peter Tippett explained that if a transcription company sent a document to Dr. Smith at Mercy Hospital, and Dr. Smith at Mercy is on the exchange, then the document would arrive properly. If the doctor did not have an account at that hospital, or if the hospital did not have an account in the exchange, then the doctor could use an online access portal that Verizon will be providing. All doctors will have rights to use this portal at no cost to them individually. Therefore, the document will reach the doctor’s account. The doctor can log in with a universal medical identity provided by Verizon. In this way, Verizon hopes to encourage people to engage more in the integration of EMRs and health information exchanges.

Peter Tippett discussed authenticating machine-to-machine endpoints: Verizon runs a certification of each endpoint with a series of testing, questionnaires, and other activities that are part of Health Insurance Portability and Accountability Act (HIPAA) related security testing. They also make sure that the application does indeed belong to Mercy Hospital by checking to see if it is there. Verizon issues a unique SSL certificate and toolkit that allows the software to join the exchange. Each endpoint has a HIPAA agreement that allows information to get where it needs to go.

Verizon uses a RESTful protocol, over HTTP, with an SSL tunnel operating at all times. The tunnel cannot connect without the identity known of the machines connecting. ITT XPR protocol will be supported by January. The identity for people who come to the provider portal is a level-3 credential that has been issued to virtually all doctors and nurse practitioners and physicians assistants in the country.

Regarding confirmation of receipt, Peter Tippett explained that all messages are hashed, all hashes are signed, and machine-to-machine protocols allow logging to know whether a message was received by machine or whether it was actually Dr. Smith who received the message. He added that Verizon has analyzed computer crimes in the last 7 years, and a combination of SMime and SMTP would have resisted every attack examined. He concluded his remarks by noting that encrypting content that is running through an encrypted tunnel adds no value at all, as long as the identity of the recipient is known.

A committee discussion followed, which included these highlights:

- Peter Tippet commented that both a yellow pages and a white pages-type directory is important. Verizon's fundamental directory is based on individuals, but connected to institutions. For example, Dr. Smith is Dr. Smith as an individual. There is also a persona of Dr. Smith as a doctor; a persona as a doctor at Mercy; and a persona as a doctor at the VA. The doctor can have multiple personas, one representing each of his professional affiliations. Each time an institution joins, it declares all of the providers it represents. The same is true with transcription companies, or whatever endpoint might be part of an exchange.

- Arien Malec commented that in the Direct Project, they found it was difficult to use DLS without some well-known root credential that everyone can prescribe to. When considering the challenge of a higher security environment, they moved to content-based security, and a mechanism that is fairly well published for how to discover mutual trust in a security negotiation during transfer. This relates to addressing in that, if one has an address, the actual connection is organization to organization. Because of how the Web works, one does not know whose machine it is before that transaction is sent. As a result, trust and addressing end up being very closely coupled.

- Peter Tippet commented that he does not see any reason why the root certifications that are trusted for commerce cannot be trusted for medical information transfer (they are used for nuclear launch codes, he noted). They are distributed, trusted by governments and technology companies, and already deployed in all technologies, including all browsers, operating systems, telephones, and some mobile telephones. He suggested that inventing a different root system likely is not necessary.

- David McCallie asked if Verizon's network is address-compatible with the Direct network. Peter Tippett replied that it is not at present, but Verizon plans for it to be interoperable with Direct both through XDR interfaces and also a traditional HIE, NHIN Direct-oriented connection. He expects that within a month or two, it will be connected to the rest of the NHIN Connect-related system, and from there, to anywhere else.

- Dixie Baker asked, when Verizon issues machine certificates, whether the company cares whether those machines are EHR servers, Web servers, or some other type of machine. Peter Tippett explained that so far, the endpoints Verizon anticipates are EHR-like machines. They might be called "document management systems" or something similar, but their function is to store data about patients in some way for access by doctors. Those machines are being certified by ICSA labs, or an equivalent. Verizon is requiring that they be certified, and that is the mechanism for controlling the problem Dixie Baker described.

- In response to a comment from John Halamka, Peter Tippett noted that Verizon has a toolkit, training guide, and other materials in various unfinished forms, and Verizon can determine which parts would be most useful to share with the Committee.

- Arien Malec asked Peter Tippett whether he believes that the processes related to identity management that e-commerce provides are sufficient for health care. Peter Tippett indicated that he did not believe this to be the case. However, the root certifications are well done, and tested by various organizations annually. SSL certifications can be obtained online with no reviews. Therefore, Verizon is insisting on certifications on the endpoints that it is providing, which includes machine penetrability vulnerability testing, and a physical visit of the machine to make sure it is in the right place.

John Feikema, Visionshare

John Feikema shared four principles in Visionshare’s approach to building healthcare communications: (1) use the ubiquity and affordability of the Internet; (2) build security into every facet of communication; (3) bulletproof scalable business practices and tools around user identity verification; and (4) increase network participation and adoption by providing a variety of on-ramps, making technology solutions transparent. Visionshare makes sure that each endpoint uses an X509 certificate, and a TLS handshake protocol is used in all cases. The Visionshare network is secured by X509 certificates and private keys. A valid government-issued picture ID is necessary to obtain certification.

Visionshare’s architecture is similar to that of the Direct Project. Visionshare plays the role of the health information service provider (HIST), meeting the provider where he or she is today, and working towards future needs. All of Visionshare’s existing Endshare users will be able to connect in a Direct-compliant way. Visionshare also has modeled Connect as an edge protocol on its network and is currently engaged in deploying a Connect gateway. The company’s customers will use the existing network capability to securely transmit documents to its gateway, which will in turn relay them to the CMS gateway.

Visionshare anticipates integrating the Direct project in a similar manner, and may use Direct as a provider protocol to submit information to a Connect endpoint at the CMS. The company has proven that a PKI-secured network, processes, and technologies can be deployed on a wide scale successfully. Ninety-four percent of Visionshare customers renew year to year, with the remaining six percent not renewing largely due to mergers and acquisitions.

John Feikema commented that semantic interoperability is a challenge, and Visionshare is pleased with the work that the HITSC has already done in this area. He added that Visionshare has learned that there is no need ever to compromise on ensuring privacy, authentication, and message non-repudiation. Placing PKI technology at the center of these efforts is important, and there is a need to clearly state and enforce requirements for securing data at rest. Also, creating standards for direct exchange around endpoint addressability and security is critical, and the Direct project is an important component to this. Finally, it is important to enable simple but secure on-ramps that hide technical complexity for the end user without sacrificing security. Providers must be given tools that do not force them to scrap legacy systems, and they must have help in solving problems of semantic interoperability. He commented that the Direct Project goes a long way towards meeting these requirements.

The Committee discussion that followed included these points:

- Wes Rishel said that, regarding semantic interoperability, Visionshare appears to be progressing on a path of incrementalism, which he strongly favors. Making the connection, and getting the data there somehow is better than not getting it there at all. As they roll out on a national level, and as EHRs roll out, issues of semantic interoperability will become increasingly important. He emphasized that it is important that they not strangle themselves with hyper-semantic interoperability. They must find a way to introduce it so that different users and systems that are at different stages in the life cycle can continue to operate. They also must recognize that NHIN Direct presents different use cases for interoperability than does NHIN Connect.

- John Feikema confirmed that users on the Visionshare network have universal addressability with other Direct users. Visionshare has already integrated the Direct protocol as an edge protocol on its network, making it a gateway. Visionshare now is an edge protocol to Direct, rather than vice versa. Visionshare mapped a way to bridge between those two using a standard Direct e-mail address.

- John Feikema suggested that the most significant issue around the certificate mechanism is going to be the policies under which those certificates are issued. The technical mechanisms are going to be fine; the challenge will be the trust fabric.

- John Feikema explained that when a user signs up they are presented with a BAA that they sign and send back, and they are also presented online with a template that describes what Visionshare knows about them already (based on information learned during the sales call, etc.). The user augments this, prints it, has it notarized (which is where the identity is checked), and sends it in. Then they are live.

- In response to a question by Wes Rishel, John Feikema explained that the kinds of use cases that the network is used for are mostly administrative transactions, many of them to Medicare. One long-time trading partner is the Minnesota Department of Health. That work involves a great deal of routing of HL7 traffic for immunizations, newborn screenings, and disease reporting.

- Dixie Baker asked how Visionshare credentials departments and business systems. John Feikema explained that the department head or person responsible for the system fills out the form and attests that they are responsible for their department and institution. He confirmed that certifications for machines are identical to certifications for people.

Joseph Carlson, Covisnt

Covisnt provides messaging services and deals with the integration of organizations across many markets: automotive, health care, oil and gas, and government. Joseph Carlson’s remarks focused on secure point-to-point transactions as well as system-to-system messaging.

Secure messaging encompasses protocol translation, integration, and all of the policy centered on transmission. Covisnt hosts all end points, and has established trading partner relationships that drive the flow of data and the ways in which they route and manage communication channels.

Whether HTTPS, secure FTP, or other protocols, there is a standard method within the applications through which users and support staff can manage the work. He emphasized that a large part of their work is being flexible: they must meet users where they are, with their existing investments in technology, etc. They may start down the road with an approach towards NHIN Direct, but Joseph Carlson noted that it comes back to what Covisnt can do today to get providers on board as soon as possible.

He discussed the specifics of authentication and management of the security of endpoints. In terms of how Covisnt configures trading partner profiles, the important concept to understand is the transport protocol and authentication criteria. When considering channels for each training partner, Covisnt can, for example, confirm that Dr. Smith is communicating over this secure transmission, and all of the associated technical details—it is not something that the end user has to worry about. Many third-party sites and open sources are supported within Covisnt's platform; the company does not need to "reinvent the wheel" or duplicate efforts every time it comes to a new endpoint.

Joseph Carlson explained that Covisnt Scout Technology is a software tool that enables providers to go to a site, download an application, and install it. Covisnt gains remote access to their system such that, out of the box, they have secure point-to-point transport over the Internet. Then, Covisnt they works with the vendor to establish back-end integration into their EMR, PMS, etc. The focus is on system-to-system messaging.

With regard to ensuring that information is not changed en route, Covisnt supports the standard digital signatures as well as the various messaging protocols in use today. Their approach is to build this "pipe" first and then manage it on both ends.

Over the last 10 years in working with endpoints, Joseph Carlson noted that he has observed that point-to-point messaging can be very costly on a continuing basis. What is the cost of maintaining this on an ongoing basis, as the number of endpoints grows? How will they manage that and be responsive to changes? This is a formidable task for organizations—one that is not just about up-front costs, but also about a continual investment in technology and meeting new requirements and standards.

The discussion following his presentation included the following points:

- David Lansky explained that the goal of the Direct Project—by trying to create an open approach—would be to enable a situation in which, for example, a user on the Verizon network who knows the address of someone hosted on Covisnt could securely deliver a message. He asked Joseph Carlson if he believes that it will be possible to avoid having to hand-craft individual solutions between two vendors. Joseph Carlson commented that this is certainly possible, and is something Covisnt is supporting. The next step after dealing with addressing and domain name would be tackling scenarios such as when a small provider is sending a CCD. The small provider likely does not know how to create CCDs, so they use an EMR to create it. How some of these back-end interfaces will work is a challenge.

- Summarizing a comment by Arien Malec, John Halamka said that if there could be one approach to trust management (even if it is a federated approach), and one approach to directory services, then all of these companies could drive endpoint services, value added features, etc., and interoperability could still be achieved.

- It was noted that there are many ways that a transaction can be organized, depending on the use case.

- Wes Rishel asked about the Covisnt value-added incentive of on-boarding and determining identity of end users. Joseph Carlson offered to send materials about this incentive to the Committee.

Anand Shroff, Axolotl

Anand Shroff began his presentation by noting that Axolotl has seen a number of different approaches, from MLLP over VPN—which is most widely used today in Axolotl systems—to secure FTP, and now synchronous Web services transactions. This is becoming the preferred approach, with SAML, because there tends to be immediate feedback on abnormal activity and it supports synchronous and asynchronous transactions.

There are a number of different candidates for messaging. The RESTful approach is Anand Shroff's favorite; however, there is no standardization around a widely accepted RESTful interface. Standardization seems to be focused on SOAP transactions. A number of approaches are available, with standardization absent. The Direct effort with SMTP is now taking center stage, and Axolotl is supportive of this move. It has the advantage of using a widely available tool set, and importantly, it allows the small providers to communicate. Outside of the push use case, SMTP is going to fall short, and this was a concern widely voiced in the NHIN Direct Workgroups. The use cases that they encounter are mostly referrals, transitions of care, discharge summaries, result exchanges from labs, and public health reporting.

With respect to NHIN Connectivity, Axolotl has built and maintains a gateway that supports NHIN protocols. Axolotl expects a number of projects to connect over the NHIN over the next 12 to 18 months. Axolotl advocates NHIN Connect-style exchange-to-exchange CCDs to exchange information across systems.

Axolotl also maintains its own provider directories. It does they do not currently support the NHIN Direct protocol, but it is expected that their directories will be able to support that kind of communication.

The committee discussion that followed included these highlights:

- With regard to the question of white pages or yellow pages-style directories, Anand Shroff commented that the most obvious answer is the hardest to accept—centralized management would be a more efficient way of doing things, versus a distributed system. Although a centralized system may not be acceptable for a number of reasons, it is the easiest and most manageable solution.

- Connie Williams noted that the Information Exchange Workgroup just discussed this issue, and arrived at a consensus about the difference between requiring people to use a specific set of rules but keeping it federated, versus actually having a centralized directory of data.

- Anand Shroff explained that with a federated approach, the ability to search will be a challenge. It could be handled with a directory of directories, but it remains a complex problem to solve. A centralized approach, does suffer from the "single point of failure" problem, but that problem has largely been addressed with redundancies, etc. Neither approach is the absolute right answer, but for simplicity and the ability to move the Direct effort forward rapidly, he prefers the centralized approach.

- Arien Malec commented that it is useful to have a common definition of identity and trust, and a well-known set of trust anchors. This follows the theme that transport is less essential than common definitions of trust. To the extent that they can get federal, cross-state definitions of trust, they will be able to scale up interoperability.

- Wes Rishel noted that technology providers are paid to take care of technical details. He suggested that perhaps user difficulties in working with technology are a problem, or perhaps they are a business opportunity for a certain type of business provider. A balanced approach is needed—there are always practical reasons why using one product would in theory be easier to coordinate, but that solution has limitations of scale, because of vendor and marketplace limitations. A balance is needed between what is practical and open versus what is solved more easily by being proprietary.

Cris Ross, Surescripts

Cris Ross highlighted the importance of point-to-point messaging for e-prescribing, noting that Surescripts is now they are adopting this for clinical interoperability. Surescripts maintains one of the largest health information networks today, with e-prescribing as its anchor service.

Approximately 65 percent of patients in the United States are searchable for prescription information. That gap is largely made up of people on Medicaid; Surescripts is in the process of adding that information to the system. Essentially, almost every meaningful piece of clinical technology is connected to the Surescripts network. In October, they transmitted more than 190 million transactions.

Part of reason they been able to reach their level of ubiquity is a set of principles under which Surescripts operates around security and privacy (these are listed in Surescripts' written testimony). There is a concept of neutrality, in which all players get to play on a level field, with the same access to e-prescribing. Surescripts expects to extend that neutrality into clinical interoperations.

Cris Ross commented that the Direct Project at this point does not produce a full sense of interoperability; it focuses only on transport, as it should. In the e-prescribing world, there has been codification of content and vocabulary over time. Lessons that were learned in the pharmacy and medications domains may be transferable to clinical exchange and may inform the Standards Committee as it proceeds.

Surescripts expects to connect to emerging and existing networks on a peer-to-peer, neutral basis. Cris Ross emphasized the critical importance of the trust model. How can a person get credentials, and then what can they do with those credentials? Trust in directories can make a critical difference. Also, trust can mean capability certifications. In this instance, Surescripts hopes to keep pace with the standards and approaches that are implemented by the HIT Policy and Standards committees. Practical experience across the Surescripts and other networks should be a learning environment that these Committees can use. Surescripts does not currently support the Connect architecture because, but Cris Ross expects that to change in the future.

The discussion that followed included the following points:

- Cris Ross noted that the ideal of a universal address does not mean a universal directory. The issue is going to be how to connect between directories. Surescripts' approach is to have a directory exchange. If a network connects to Surescripts, there is a way to receive information around that directory that would make it searchable within their domain. He does not think there is a protocol for that today.

- Arien Malec pointed out that in the e-prescribing network, development has been characterized by a few large players. It is similar to the credit card industry, in which there are three large card issuers. In the clinical exchange world, there are more large networks than existence than there are in the world of pharmacy aggregators. He asked how those network dynamics inform the trust and standards that Surescripts uses, and how those things might change with a wider variety of networks participating. Cris Ross commented that vendors who serve small providers often provide aggregation service on behalf of individual prescribers. The individual doctor's office is not managing the technology; the EHR vendors are doing that on behalf of those individuals. In extreme situations, such as when individual physicians need to manage all of the infrastructure and the business of connecting to their peers, that is a significant burden. In reality, the industry has generated opportunities for vendors to provide those services. He expects to see the same phenomenon outside of e-prescribing (all of today's presenters are offering to do that job).

Eric Dishman and Gary Bender, Intel

Eric Dishman emphasized the need to ensure that use cases include home care, family members, community health workers, and a range of medical and consumer devices. These are all components that need to be included in infrastructure.

Eric Dishman's social science team at Intel has studied health care facilities around the world, with a particular focus on their adoption (or lack thereof) of EHRs. Intel supports NHIN Direct, and his group is incorporating some of these security technologies right into Intel products. They are also working with health care providers on health IT strategies for becoming connected users. Eric Dishman commented that secure data exchange between health care providers of any size is doable and achievable.

Gary Bender reported that Intel has spent a significant amount of time implementing e-commerce solutions. It also has done some work recently with point-to-point solutions, particularly with regard to transmitting information back and forth between home devices and a central depository, and even into an EMR.

In terms of transport, Intel uses Web services extensively in their work. Gary Bender said he understands why SOAP and REST are very useful and popular. As an architect, he sees their benefits; as a systems integrator, he understands why it is good to have those data transfer capabilities in place. However, if they took a survey, 4 out of 5 physicians probably have no idea what SOAP and REST are. From a clinical perspective the question is, how can we get data in and out quickly, effectively, and without having any in-depth technical know-how? The point is for these systems to be utilitarian in nature. Users want to treat these systems and services as "plumbing," and not have to understand them.

With respect to authentication, Gary Bender said he agrees with the direction of this meeting's discussions. There is an ongoing philosophical discussion about the granularity of digital identities, and he offered two rules of thumb:

1. Digital identity should accurately reflect the source of the data. So if the data were a message from a doctor to the patient, he would expect that the message would be signed by the digital identity of the doctor. If the message includes extensive medical history about a patient, he would expect that to be signed by the digital identity of the EMR. The signature depends on the nature of the data being sent.

2. Granularity in moving these digital identities out to the endpoints makes good sense. They do not want to move to the point where every individual is required to have a digital identity where there is no reason for it. However, moving in that direction as time and technology allows does make sense (but does not trump the first rule of thumb, which is that the signature needs to accurately reflect the source of the data).

Digital signatures are ubiquitous enough that using a non-repudiating receipt makes sense. Gary Bender suggested that the solution be built on existing, known standards. He urged the Committee to carefully choose the standards that are going to be simple, clear, and meet the needs of the community.

In discussion, the following points were made:

- In response to a question about implications for the device world of consumers having an address that maps to their data home or their personally controlled health record, Eric Dishman said that it depends partly on whether or not the data is going to a clinician. He explained that we are quickly moving to an environment in which levels of trust are assigned and assumed depending on the answer to questions like, "Is this 'real' health data because it comes from my doctor, or 'not real' because it comes from my PHR?" The same concept will hold true for peripheral medical devices. Those data sources will need to be identified and prioritized.

- With regard to unattended home health care, Wes Rishel asked about the requirements of extremely high bandwidth for some devices. Eric Dishman noted that the first issue is what determining the class of the device. If it is a monitoring device not intended for intervention in critical situations, then there are some options. There could be a significant benefit with a more robust connection, but it is not necessarily critical.

- To extrapolate this out to the future, Eric Dishman said, they are going to want the ability to prioritize data that goes to, for example, the heart monitor, versus less critical functions. Intel has a model that sorts out what someone can do on their own, versus things that can be done by a community member, versus things that a full-blown medical professional could do in the home. Some patients are already doing home dialysis without a medical professional present. Intel is working with many governments in the world who believe that there are not going to be enough resources to not have this type of care. He acknowledged that more study is needed on these issues, and expressed hope that the United States will adopt that position as well.

6. HIT Standards Committee Discussion and Next Steps

John Halamka explained that the next step for the Committee is to evaluate the Direct Project on its own merits. Is the implementation guidance provided by that project simple, direct, scalable, and secure, to meet the goals articulated?

Peter Tippett cautioned that the world is moving to cloud computing. If the Committee insists on end-to-end encryption of messages, depending on what is called the "end," it may be impossible to use the cloud infrastructure. Therefore, the pipe infrastructure plus a well-authenticated end user may be necessary. He added that it is likely that every vendor at this meeting has a cloud-based future and current applications, and users are getting to them with some sort of device that does not necessarily need to be "smart." He also noted that he cannot imagine the improved value of keeping the message encrypted in addition to the pipe.

Dixie Baker explained that the trust fabric is essential, much more so than the method of the transport. From this testimony, she learned that that trust fabric needs to include common policies for managing the X509 certificate for both people and software, and it must also include policies having to do with managing directories. She was surprised to learn that certificates are being issued to people, departments, and servers. That variety of certificate use and the variety of policies relating to their issuance is an important value coming out of this testimony, and points to the need for uniform policy there.

Dixie Baker also stressed that a common policy about data integrity protection and non-repudiation of receipt is needed. None of these are required by the Health Insurance Portability and Accountability Act. It does not seem necessary that everyone use the same transport protocol, although there will need to be agreement between two endpoints. Finally, she was reminded at this meeting that the endpoint address may not be routable, and there is a need to consider alternative protocols for this.

David Lansky said that a case could be made that some of the information presented at this meeting describes a scenario that is not very different from universal addressing in e-mail. He pointed to the old AOL/CompuServe/local enterprise “soup” of incompatible mail systems. With the emergence of a definition of SMTP, that slowly gave way to true universal addressing. They are poised to see the same thing now with secure messaging.

Wes Rishel noted that the Committee is constantly trying to maintain two trains of thought—a vision of the future, and what can be done in the timeframes of the various meaningful use deadlines. It is helpful to know that there are individual certificates being issued and that at the same time, there is a need to recognize the accelerating nature of using certificates related to organizations and letting the organization be responsible for individuating the actual recipient via the department or person, based on internal rules.

Wes Rishel also commented that there are three levels to consider when looking into the importance of not losing the value of the cloud. One level is point-to-point transmission, and the purpose of the cloud is to enable that transition, with the ideal situation being that the cloud entity has no knowledge of the content. A compromise level is to acknowledge that there is a need to decrypt and re-encrypt in order to match protocols, but no retention of information in the cloud. In the third level, by virtue of retaining information in the cloud as it is passed through, there is value added. In this situation, a critical issue is that patient consent be invoked.

7. Public Comment

There were no comments from the public.

SUMMARY OF ACTION ITEMS

Action Item #1: Minutes from the last HITSC meeting, held on October 27, 2010, were approved by consensus with the addition Cammie Roberts’ e-mailed response to Committee members.